IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA,	)	CR 17-00109 LEK
	)	
Plaintiff,	)	
	)	
vs.	)	
	)	
MICHAEL PHILLIP PATRAKIS,	)	
	)	
Defendant.	)	
_____	)	

ORDER DENYING DEFENDANT MICHAEL PATRAKIS' MOTION TO SUPPRESS EVIDENCE, FILED APRIL 20, 2017 [DKT. NO. 53]

The evolution of technology gives rise, in this particular case, to the question of whether a third-party's access to a defendant's personal home surveillance system stored in the cloud (that is, where managed remotely and made available to users over the internet)[1] requires law enforcement first to obtain a search warrant before accessing, downloading and copying the digital video content. Under the facts of this case, an authorized user accessed the account containing the video content and showed it to the police. Therefore a warrant was not required.

Defendant Michael Patrakis ("Defendant") filed his Motion to Suppress Evidence ("Motion") on April 20, 2017, [dkt.

[1] "Cloud computing refers to applications and services offered over the Internet. These services are offered from data centers all over the world, which collectively are referred to as the 'cloud.'" *Cloud Computing*, The Tech Terms Computer Dictionary (April 23, 2009), https://techterms.com/definition/cloud_computing.

no. 53,] and the evidentiary hearing, pursuant to Franks v. Delaware, 438 U.S. 154 (1978), was held on November 15, 2017. He seeks to suppress video and physical evidence obtained by law enforcement. Two police officers and Defendant testified at the hearing.

For the reasons set forth more fully below, the Motion is denied because an authorized third party consented to provide access to law enforcement to Defendant's home surveillance video account. The surveillance video content constituted probable cause for the subsequent entry into Defendant's home without a warrant to remove any minors and assume their protective custody. During the entry, certain physical items were observed in "plain view" and permissibly supported probable cause for a search warrant for Defendant's residence as well as the other search warrants issued for Defendant's computers, cellular telephones, cameras and websites that may have been accessed by him. Even if these observations are excised from the affidavit, ample probable cause still existed for the warrants to issue.

BACKGROUND

The facts pertinent to the background of this case are: A five-count criminal indictment was filed against Defendant on February 23, 2017. [Dkt. no. 41.] These charges are based upon evidence obtained by law enforcement: (1) video seized from Defendant's video surveillance system without a search warrant;

(2) police observations made during a warrantless entry into Defendant's residence; and (3) physical evidence recovered pursuant to search warrants issued based on the video content seized, and observations made during the warrantless entry.

At approximately 3:00 a.m. on September 17, 2015, a witness met with local police to report child abuse. [Gov't Hrg. Exh. 1 (Search Warrant No. 2015-132K filed September 21, 2015), Aff. of Officer dated September 18, 2015 ("9/18/15 Aff.") at 000154.[2]] During the initial and subsequent meetings with police that day, the witness accessed Defendant's DropCam account for his video home surveillance through the internet and showed the video content to police officers.[3] [Id. at 000160-61.]

Additionally, she told the police officers that: (1) the surveillance video depicted recent events which took place in Defendant's home and master bedroom; (2) Defendant gave her Defendant's username and password for his DropCam account; and (3) Defendant gave her permission to view the online video content in his DropCam account. [Id. at 000154-55, 000160.]

---

[2] The 9/18/15 Affidavit was prepared by Sharlotte T. Bird, a detective with the Hawai`i Police Department. [9/18/15 Aff. at 000153.]

[3] DropCam is a commercial product which offers wi-fi wireless video monitoring through a security camera which streams video images that are accessed on the internet at the DropCam website by a user through a DropCam account. The witness told the detective that these images are stored remotely "in a place like 'iCloud' and the information is deleted every 10 days." [9/18/15 Aff. at 000160.]

Defendant denies giving the third-party witness permission to access his DropCam account.

Copies of the online videos in Defendant's DropCam account were transferred by the witness onto two CDs and a thumb drive, then given to the police. [Gov't Hrg. Exh. 3 (CD containing videos recovered on 9/17/15 at the Kealakehe Police Station); Gov't Hrg. Exh. 4 (thumb drive containing videos provided to Detective Bird on 9/18/15); Gov't Hrg. Exh. 5 (CD containing videos recovered on 9/19/15 at the Captain Cook Police Station).]

On September 17, 2015, after reviewing the DropCam account's video content and without first obtaining a warrant, the police entered Defendant's residence with Child Welfare Services to remove any children in the home, pursuant to Haw. Rev. Stat. § 587A-8(a)(1)[4]. During this entry, the police observed drug paraphernalia and a digital video recording camera in Defendant's bedroom, removed two minors from the home, and

---

[4] In relevant part, this statute provides:

> (a) A police officer shall assume protective custody of a child without a court order and without the consent of the child's family, if in the discretion of the police officer, the officer determines that:
>
> > (1) The child is subject to imminent harm while in the custody of the child's family[.]

Haw. Rev. Stat. § 587A-8(a)(1).

arrested Defendant on a state criminal charge. [9/18/15 Aff. at 000156-59.]

On September 18, 2015, a search warrant for Defendant's residence was issued based upon the DropCam account's video content shown to police by the witness, and observations made by police during the entry without a warrant. [Gov't Hrg. Exh. 1 at 000148-49 (SW 2015-132K); 9/18/15 Aff. at 000154-55, 000158-59.] Items recovered from this search included a digital scale, syringes, smoking pipes, cellular telephones, a computer, computer tablets, and digital cameras. [Gov't Hrg. Exh. 2 (Return of Search Warrant No. 2015-132K, filed on September 23, 205) at 000177, 000179, 000181-86, 000188.] Law enforcement subsequently recovered additional evidence from websites, computers, cellular telephones and cameras as a result of search warrants based on the DropCam account's video content and the fruits of the first search warrant. [Motion, Decl. of Counsel at ¶¶ j-t.]

DISCUSSION

Defendant contends that the third-party witness did not have permission to access his DropCam account, and therefore all evidence obtained as a result of law enforcement's viewing of the DropCam account's video content must be suppressed. He further argues that the witness accessed his account as law enforcement's agent and thereby triggering Fourth Amendment interests.

Specifically, he seeks suppression of: copies of the DropCam account's video content; items recovered from his residence on September 18, 2015 pursuant to search warrant SW 2015-132K; items recovered as a result of searching the computer systems of Adult Friend Finder, Adultism and DropCam by Nest Labs pursuant to search warrants SW 2015-145W, SW 2015-146K and SW 2015-147K obtained on October 1, 2015; items recovered from Defendant's computers, cellular telephones and cameras pursuant to search warrant SW 2015-148K, obtained on October 5, 2015; and items recovered from Defendant's cellular telephone pursuant to search warrant SW 2015-177K filed, obtained on December 8, 2015. [Id.] If, as Defendant argues, the third-party witness had no authority to access for law enforcement and make copies of the DropCam account's video content, then the subsequent warrantless entry and search warrants are all tainted and the evidence must be suppressed.

Plaintiff United States of America ("the Government") submits that: Defendant did not have a reasonable expectation of privacy in the video contents of the DropCam account; the witness had actual or apparent authority to access the DropCam account; the search was by a private citizen (the witness) and not law enforcement, and thus did not require a warrant; the searches of the DropCam account were justified by exigent circumstances (*i.e.*, account video content is erased every ten days); the

warrantless entry was justified by exigent circumstances (namely, the video content demonstrated imminent harm to minors); and the search warrants were supported by probable cause independent from any observations made during the warrantless entry.

Whether the entry into Defendant's residence without a warrant and the subsequent searches were permissible rise or fall on a single determination: did the witness have authority to access and display Defendant's DropCam account's video content? She did.

I. DropCam Account

Defendant had a legitimate, reasonable expectation of privacy for the contents of his DropCam account. See United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (citing United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers.")); see also United States v. Buckner, 473 F.3d 551, 554-55 n.2 (4th Cir. 2007) (recognizing a reasonable expectation of privacy in the defendant's password-protected files on a computer leased by his wife); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (same as to a computer the plaintiff and another person had joint access to)). He had a specific account which required a user name and password; without the required information, no one could access

the DropCam account's content.[5] Metaphorically speaking, Defendant installed a door and lock on his computer account. The witness had Defendant's user name and password for the DropCam account; that is, she had his key to unlock the door and access the account's content. "A third party's consent to the search of another's belongings is valid if the consenting party has either actual or apparent authority to give consent." United States v. Ruiz, 428 F.3d 877, 880 (9th Cir. 2005) (citing United States v. Davis, 332 F.3d 1163, 1169 (9th Cir. 2003)). Actual authority in this instance would entail Defendant expressly authorizing the witness to give consent or if the witness had mutual use of the DropCam account and joint control or access to it. See id. (quoting United States v. Fultz, 146 F.3d 1102, 1105 (9th Cir. 1998)).

Defendant testified that he did not give permission to the witness to access his DropCam account. His testimony was not directly contradicted because the witness did not testify. Ample evidence supporting actual authority to consent to search however

[5] In stark contrast, a peer-to-peer network permits files located on one individual's computer to be shared with other members of network as long as the person seeking the files is connected to the internet and has peer-to-peer software. *P2P*, The Tech Terms Computer Dictionary (2006), https://techterms.com/definition/p2p; see also United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) ("[H]e was explicitly warned . . . that the folder into which files are downloaded would be shared with other users in the peer-to-peer network.").

was given by police officers' testimonies that: the witness stated that she had Defendant's permission to access the DropCam account; she stated that she was Defendant's close friend; she possessed both the user name and password; and she was able to access Defendant's DropCam account in the officers' presence. On balance, the Government established that it is more likely than not the witness had actual authority to display and copy the DropCam account's contents because she had his consent or had mutual use and control.

Alternatively, if Defendant's testimony is sufficient to defeat a finding that the witness had actual authority, reliable evidence exists for a finding that she had apparent authority. The three-part test for a third-party's apparent authority to consent to search is:

> First, did the searching officer believe some untrue fact that was then used to assess the extent of the consent-giver's use of and access to or control over the area searched? Second, was it under the circumstances objectively reasonable to believe that the fact was true? Finally, assuming the truth of the reasonably believed but untrue fact, would the consent-giver have had actual authority?

Id. at 880-81 (quoting United States v. Dearing, 9 F.3d 1428, 1429-30 (9th Cir. 1993)). Here, police officers testified that: the witness said that she was Defendant's friend; Defendant gave her permission to access his DropCam account; they questioned her as to how and why she was given permission; they believed her

representation; and she was successfully able to retrieve the DropCam account video content with a user name and password. Thus, even if the witness falsely represented to law enforcement that Defendant gave her permission to access the DropCam account and this falsehood led the police to believe incorrectly that she had use, access and control over this account, the Government established that the police were objectively reasonable in believing the witness had Defendant's permission and in concluding that she had actual authority.

While the Government argues that, pursuant to United States v. Kroll, 116 F.3d 994, 997-98 (2d Cir. 1997), the Fourth Amendment's prohibition against unreasonable searches and seizures does not apply to the witness because she is a private citizen, in the event Defendant did not give permission for her search, Kroll does not apply here. In Kroll, individuals stole documents and turned that evidence over to law enforcement. The Second Circuit affirmed the district court's conclusion that these individuals were not state actors and therefore exempt from Fourth Amendment search and seizure restrictions. In contrast, the witness here did not merely search and copy Defendant's video content, and then turn those copies over to law enforcement. Instead, she gave law enforcement access to Defendant's DropCam account, and the police conducted their own searches and seizures (i.e., viewed the content on police computers and directed the

witness to make copies). "'Where a private party acts as an "instrument or agent" of the state in effecting a search or seizure, Fourth Amendment interests are implicated.'" United States v. Cleaveland, 38 F.3d 1092, 1093 (9th Cir. 1994) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487, 91 S. Ct. 2022, 2048–49, 29 L. Ed. 2d 564 (1971)), *as amended*, Jan. 12, 1995.

Ultimately, however, whether or not the witness acted as the government's agent is a distinction without a difference. Unlike the power company agent in Cleaveland who pried open, took apart and searched the meter's conduit pipe without the homeowner's permission, the witness had Defendant's permission (actual authority) or reasonably appeared to have his permission (apparent authority) to consent to search. The Fourth Amendment was therefore not implicated.[6]

II. Warrantless Entry into Residence.

Law enforcement entries into homes start with the premise "'that search and seizures inside a home without a warrant are presumptively unreasonable.'" Kentucky v. King, 563 U.S. 452, 459 (2011) (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)). "One well-recognized exception applies when 'the exigencies of the situation' make the needs of law

[6] As the Court has concluded that the witness had actual or apparent authority to consent to search, it declines to address the Government's argument that the search and seizure of the DropCam account's video content without a warrant was justified by exigent circumstances.

enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.'" Id. at 460 (alteration in King) (some citations omitted) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)).

The Government established specific and articulable facts supporting exigencies so compelling that entering Defendant's residence without a warrant was objectively reasonable. Police testimony established that Defendant's DropCam account had video content depicting the following, which occurred in his residence: Defendant ingesting substances suspected to be drugs; Defendant appearing to permit his minor sons to physically abuse a toddler; Defendant appearing to physically abuse the same toddler; and Defendant taking photographs of the toddler's genitals. Police testimony also established that law enforcement concluded from the video content that minors were in imminent harm, and believed that a warrant was not necessary under state law in order to take protective custody of the minors depicted in the video content.

III. Search Warrants and Subsequent Seizures

Following law enforcement entry into Defendant's residence without a warrant to take custody of the minors, police obtained the first search warrant. The affidavit supporting the first warrant relied, in part, on police observations made during the entry. [9/18/15 Aff. at 000158-59.] Objects seized in

"plain view" do not require a warrant. United States v. Hudson, 100 F.3d 1409, 1420 (9th Cir. 1996) (stating plain view doctrine test). The Government credibly established that, during the entry, law enforcement made observations of items in plain view but neither searched the residence nor seized any objects. Moreover, even if including these observations in the 9/18/15 Affidavit impermissibly supported the first warrant, these observations can be excised and the affidavit's remaining evidence examined to determine whether probable cause was established for the warrant to issue. See United States v. Nora, 765 F.3d 1049, 1058 (9th Cir. 2014) ("A search warrant isn't rendered invalid merely because some of the evidence included in the affidavit is tainted." (citing United States v. Reed, 15 F.3d 928, 933 (9th Cir. 1994)). After excising the observations made during the entry, the affidavit's remaining evidence (*i.e.*, descriptions of Defendant's activities as viewed in the DropCam account's video content) amply supports probable cause for the warrant to be issued. [9/18/15 Aff. at 000153-55.]

In light of the foregoing, because the search warrants issued after the first search warrant were based upon the DropCam account's video content seized by the police, and evidence seized from the search conducted under the aegis of the first search warrant, the Court concludes that all of the subsequent searches were properly supported by probable cause.

CONCLUSION

Because the third-party witness had actual or apparent authority to consent to search of Defendant's DropCam account, and the video contents of that account supported a warrantless entry into Defendant's residence because of imminent harm to minors and as authorized by Haw. Rev. Stat. § 587A-8, Defendant's Motion to Suppress is HEREBY DENIED.

IT IS SO ORDERED.

DATED AT HONOLULU, HAWAII, December 21, 2017.

/s/ Leslie E. Kobayashi
Leslie E. Kobayashi
United States District Judge

UNITED STATES OF AMERICA V. MICHAEL PHILLIP PATRAKIS; CRIMINAL 17-001009 LEK; ORDER DENYING DEFENDANT MICHAEL PATRAKIS' MOTION TO SUPPRESS EVIDENCE, FILED APRIL 20, 2017 [DKT. NO. 53]